(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 426 541 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **90403024.4**

(51) Int. Cl.5: **G06K 19/06, G07F 7/08**

(22) Date de dépôt: **26.10.90**

(30) Priorité: **03.11.89 FR 8914414**

(43) Date de publication de la demande: **08.05.91 Bulletin 91/19**

(84) Etats contractants désignés: **CH DE FR GB LI**

(71) Demandeur: **LABORATOIRE EUROPEEN DE RECHERCHES ELECTRONIQUES AVANCEES**
9, Place des Vosges La Défense 5
F-92400 Courbevoie(FR)

(72) Inventeur: **Diehl, Eric**
THOMSON-CSF SCPI Cédex 67
F-92045 Paris la Défense(FR)

Inventeur: **Hamon, Joel**
THOMSON-CSF SCPI Cédex 67
F-92045 Paris la Défense(FR)

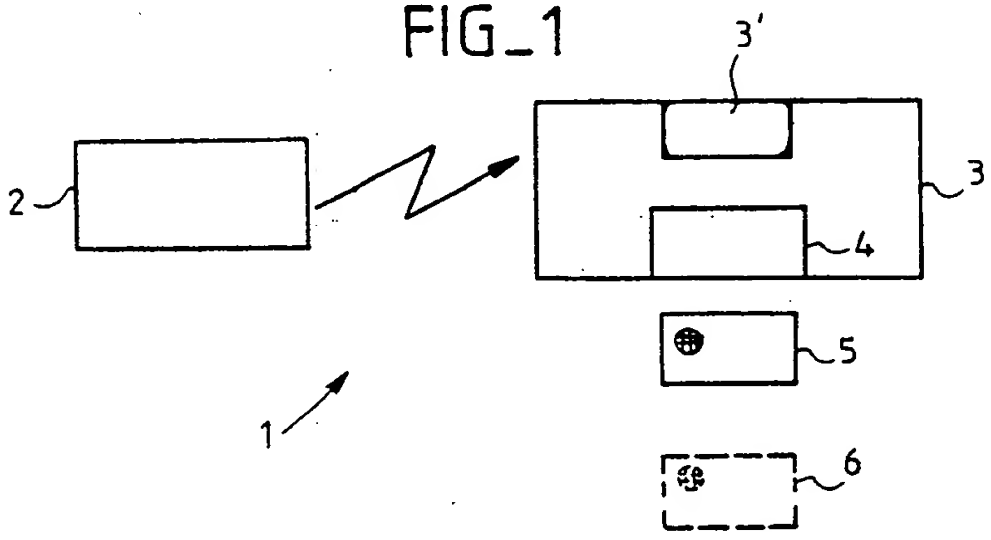
Inventeur: **Leduc, Michel**
THOMSON-CSF SCPI Cédex 67
F-92045 Paris la Défense(FR)

(74) Mandataire: **Chaverneff, Vladimir et al**
THOMSON-CSF SCPI
F-92045 PARIS LA DEFENSE CEDEX 67(FR)

(54) Procédé de protection contre l'utilisation frauduleuse de cartes à microprocesseur, et dispositif de mise en oeuvre.

(57) Pour éviter qu'une personne ayant trouvé une carte d'abonnement (5) de télévision à péage, ou l'ayant volée, ne l'utilise frauduleusement, on inscrit dans une zone protégée en lecture et écriture de la carte l'identité de l'abonné. Au début de la période d'utilisation d'une nouvelle carte (6), l'émetteur (2) compare l'identité de la nouvelle carte à celle de l'ancienne, et ne délivre le mot de contrôle que si les deux identités sont les mêmes.

FIG_1



EP 0 426 541 A1

PROCEDE DE PROTECTION CONTRE L'UTILISATION FRAUDULEUSE DE CARTES A MICROPROCESSEUR, ET DISPOSITIF DE MISE EN OEUVRE

La présente invention se rapporte à un procédé de protection contre l'utilisation frauduleuse de cartes à microprocesseur, et à un dispositif de mise en oeuvre de ce procédé.

Certains réseaux de télévision à péage nécessitent l'utilisation de cartes à microprocesseur en tant que moyens de paiement pour les prestations servies.

Ces cartes peuvent être perdues par leurs possesseurs légitimes, ou elles peuvent leur être volées. En général, ces cartes ont une durée de validité de quelques mois, afin de limiter ces risques, ainsi que les risques de contrefaçon Toutefois, en cas de perte ou de vol, la personne ayant récupéré une carte peut l'utiliser frauduleusement, et à la fin de la durée de validité peut, si elle a suffisamment de connaissances techniques, arriver à simuler le signal envoyé par le lecteur de cartes pour faire savoir à l'émetteur de programmes que la carte utilisée est encore valable.

La présente invention a pour objet un procédé permettant d'empêcher une personne non autorisée d'utiliser dans un système, en particulier de surveillance ou de distribution de biens ou de prestations, une carte à microprocesseur après la fin de la période de validité de cette carte. La présente invention a également pour objet un dispositif de mise en oeuvre de ce procédé.

Le procédé de la présente invention consiste à attribuer une identité à chaque utilisateur et à la mémoriser dans les cartes qui lui sont délivrées et à vérifier à la fin de la période de validité d'une carte à microprocesseur, lors de son renouvellement que la nouvelle carte a la même identité que la carte précédente.

Selon un aspect du procédé de l'invention, on réserve dans les cartes au moins un champ dans lequel on mémorise des données uniques relatives à l'identité de l'utilisateur et on vérifie dans la carte que lorsque l'utilisateur met en service une nouvelle carte, ledit champ de la nouvelle carte est le même que celui de l'ancienne carte.

Le dispositif de l'invention est un réseau, en particulier de distribution de biens ou de services, comprenant au moins un centre de gestion ou émetteur et au moins un terminal, dans lequel le terminal comporte des moyens permettant de mémoriser le contenu crypté d'un champ donné d'une première carte à microprocesseur utilisée dans un terminal donné, et des moyens pour envoyer vers une seconde carte ledit contenu mémorisé.

La présente invention sera mieux comprise à la lecture de la description détaillée d'un mode de réalisation, pris comme exemple non limitatif et illustré par le dessin annexé sur lequel :

- la figure 1 est un bloc-diagramme simplifié d'un réseau conforme à l'invention, et
- la figure 2 est un diagramme de champ d'identification d'une carte à microprocesseur utilisée dans le réseau de la figure 1.

L'invention est décrite ci-dessous en référence à un réseau de télévision à péage, mais il est bien entendu qu'elle n'est pas limitée à une telle application, et qu'elle peut être mise en oeuvre dans tout réseau tel qu'un réseau de surveillance de biens et/ou de personnes ou un réseau de distribution de biens ou de services (réseau de distributeurs de billes de banque ou de spectacles, d'essence, de caisses enregistreuses de magasins ...). Un tel réseau comporte au moins un centre de gestion (ou serveur) ou un émetteur, et au moins un terminal approprié pouvant être proche ou distant du centre de gestion ou de l'émetteur, ce terminal comportant des moyens pouvant coopérer avec des cartes à microprocesseur.

Le réseau 1 de télévision à péage de la figure 1 comporte un émetteur 2 et plusieurs récepteurs. Pour simplifier le dessin, un seul récepteur, référencé 3, a été représenté.

Ce récepteur 3 comporte un dispositif d'affichage 3', qui peut être l'écran de ce récepteur. On n'a représenté dans le récepteur 3 que le seul dispositif nécessaire à l'exposé de l'invention, à savoir un lecteur 4 de cartes à microprocesseur (connues sous l'appellation de "smart card"). Ces cartes peuvent comporter, en plus de leurs circuits habituels, des jonctions fusibles ("jetons") qui représentent un crédit d'émissions, et qui sont grillées au fur et à mesure de l'utilisation de carte.

On a représenté en figure 1 une première carte 5 (en traits pleins) qui représente la carte dont la période de validité vient de s'achever, et une deuxième carte 6 (en traits interrompus) qui représente la nouvelle carte correspondant à la période de validité suivante.

Les cartes 5,6 comportent de façon habituelle, dans leur section de mémoire inhibée en lecture et en écriture, plusieurs champs de données secrètes. Ces données secrètes sont par exemple le numéro d'identification de la carte, le numéro de compte en banque de l'utilisateur, son crédit permis, un algorithme de décryptage...

Une de ces sections est représentée en figure 2, et référencée 7 pour la carte 5 et 7' pour la carte 6. Cette section 7 (7') est réservée à des données d'identification de la carte. Cette section 7 (7') comporte deux champs 8,9 (pour la carte 5) et 8',9' (pour la carte 6). Le champ 8 (8') comprend

des données représentant des paramètres de validité (période de validité...) ou de personnalisation de l'abonnement pour lequel est émise la carte (genre d'émission, durée,...). Le champ 9,9' contient un code d'identification de la carte et/ou du porteur.

En outre, la section 7,7' contient un champ 10,10' qui contient, dans le présent exemple, un seul bit. Ce champ 10,10' n'est pas nécessairement contigu aux champs 8,9 ou 8', 9'. Le bit du champ 10,10 est initialement un zéro. L'émetteur 2 vérifie que lorsqu'une nouvelle carte 6 est introduite dans le lecteur 4 au début d'une nouvelle période de validité, le bit du champ 10' est bien un zéro. Si tel est le cas, l'émetteur 2 demande à l'utilisateur (affichage en 3') d'introduire dans le lecteur 4 l'ancienne carte 5 pour avoir connaissance de son champ 9 et le mémoriser, puis demande à l'utilisateur de réintroduire dans le lecteur 4 la carte 6, et envoie à la carte 6 le champ 9. Si la carte 6 constate qu'il y a identité entre ces deux champs, la carte 6 autorise le décodeur du lecteur 4 à commander l'inscription d'un "1" dans 10' et peut alors fonctionner normalement, c'est-à-dire qu'elle délivre le mot de contrôle au récepteur 3 pour lui permettre de désembrouiller les programmes embrouillés, pendant toute la durée de validité de la carte 6. Sinon, le lecteur commande l'affichage en 3' d'un message de carte non valable, et la carte ne peut pas envoyer le mot de contrôle et peut être inhibée de façon définitive. Ainsi, selon la présente invention l'identité encryptée de l'ancienne carte 5 est provisoirement mémorisée dans le lecteur 4 (où elle est accessible de l'extérieur, mais du fait qu'elle est encryptée selon le concept de connaissance nulle "zéro knowledge", on ne peut pas retrouver cette identité), puis envoyée à la nouvelle carte 6. L'identité de la nouvelle carte ne peut être transférée vers le lecteur 4 que si cette carte a été validée, donc reconnue bonne.

On notera que si l'utilisateur effectue le changement de carte en cours de fonctionnement du récepteur 3, celui-ci garde en mémoire la valeur du champ 9 de la carte 5, et lorsque l'utilisateur enlève la carte 5 pour la remplacer par la carte 6, cette carte 6 est initialisée (inscription d'un "1" dans le champ 10') automatiquement si elle est valide, c'est-à-dire si le contenu de son champ 9' est identique au contenu du champ 9 de la carte 5.

Selon une variante, on peut prévoir un champ supplémentaire dans la section 7,7' comportant un numéro de code connu du seul utilisateur légitime qu'il doit composer avant l'initialisation d'une nouvelle carte.

Ainsi, selon la présente invention, l'autorisation de mise en service d'une carte est indépendante de l'obtention du mot de contrôle, dans le cas d'un réseau de télévision à péage.

Revendications

1. Procédé permettant d'empêcher une personne non autorisée d'utiliser dans un système de distribution de biens ou de prestations, ce système comportant au moins un centre de gestion et au moins un terminal relié à ce centre, une carte à microprocesseur après la fin de la période de validité de cette carte, caractérisé par le fait qu'il consiste à attribuer une identité à chaque utilisateur et à la mémoriser dans les cartes qui lui sont délivrées, et à vérifier à la fin de la période de validité d'une carte, lors de son renouvellement, que la nouvelle carte a la même identité que la carte précédente.

2. Procédé selon la revendication 1, caractérisé par le fait que l'on réserve dans les cartes au moins un champ dans lequel on mémorise des données uniques relatives à l'identité de l'utilisateur et que l'on vérifie dans la carte que lorsque l'utilisateur met en service une nouvelle carte, ledit champ de la nouvelle carte est le même que celui de l'ancienne.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé par le fait que lors du renouvellement d'une carte, on vérifie que la nouvelle carte n'est pas une carte déjà initialisée.

4. Procédé selon la revendication 3, caractérisé par le fait que l'initialisation d'une carte consiste, après vérification de la possession par l'utilisateur d'une carte précédente et d'une nouvelle carte de même identité, à modifier de façon irréversible une donnée secrète de la nouvelle carte.

5. Procédé selon l'une des revendications précédentes, caractérisé par le fait que lors de la mise en service d'une nouvelle carte, l'utilisateur doit composer un numéro de code secret.

6. Dispositif de protection contre l'utilisation par des personnes non autorisées de cartes à microprocesseur dans un réseau de contrôle ou de distribution de biens ou de services, comprenant au moins un centre de gestion (2) ou émetteur et au moins un terminal (3), caractérisé par le fait que le terminal comporte des moyens permettant de mémoriser le contenu crypté d'un champ donné (9) d'une première carte à microprocesseur (5) utilisée dans un terminal donné (3), et des moyens pour envoyer vers une seconde carte ledit contenu mémorisé.

7. Dispositif selon la revendication 6, caractérisé par le fait que chaque terminal comporte des moyens commandés par la carte pour envoyer à la carte une tension d'écriture d'une information d'initialisation de cette carte dans un champ (10') de la mémoire de cette carte.

8. Décodeur pour le désembrouillage d'émission de télévision embrouillées, caractérisé par le fait qu'il met en oeuvre le procédé selon l'une des revendications 1 à 5.

9. Décodeur pour le désembrouillage d'émission de télévision embrouillées, caractérisé par le fait qu'il comporte un dispositif de protection selon la revendication 6 ou 7.

FIG_1

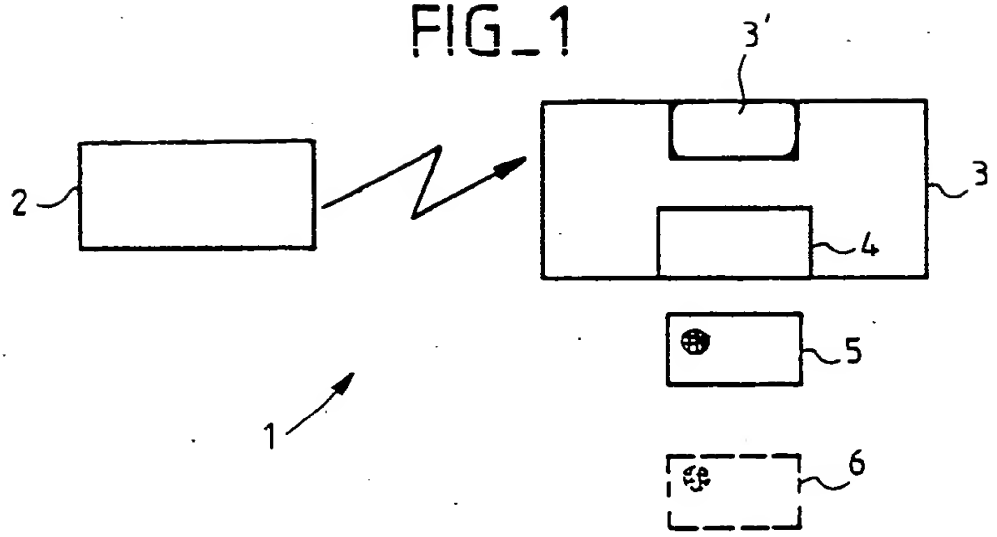
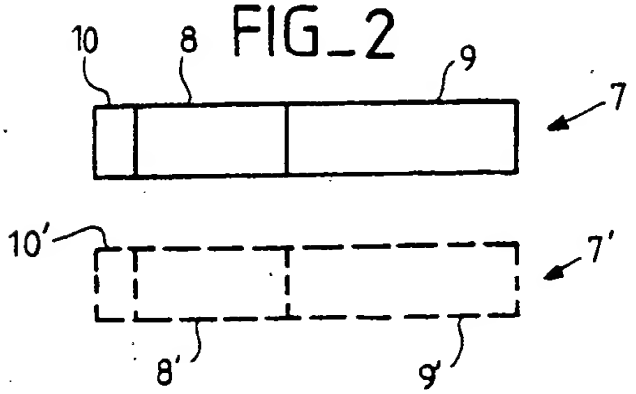


FIG_2



Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 90 40 3024

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.5)
A	WO-A-8 604 170 (BULL S.A.) * abrégé; revendications 1-9, 13-19 * * pages 1 - 2 *	1-2,5-7	G 06 K 19/06 G 07 F 7/08
A	US-A-4 367 402 (G. GIRAUD) * abrégé; revendications 1-3 * * colonne 1 - colonne 2, ligne 40 *	1-2,5-6	
A	FR-A-2 534 712 (TRAITEMENT DE L ¾ INFORMATION TECHNIQUES NOUVELLES) * pages 1 - 3, ligne 10; revendications 1, 3, 6, 11 *	1,2,6	

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
G 06 K G 07 F

Le présent rapport de recherche a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	05 février 91	BEAUCE G.Y.G.

CATEGORIE DES DOCUMENTS CITES

- X: particulièrement pertinent à lui seul
- Y: particulièrement pertinent en combinaison avec un autre document de la même catégorie
- A: arrière-plan technologique
- O: divulgation non-écrite
- P: document intercalaire
- T: théorie ou principe à la base de l'invention
- E: document de brevet antérieur, mais publié à la date de dépôt ou après cette date
- D: cité dans la demande
- L: cité pour d'autres raisons

.....

- &: membre de la même famille, document correspondant